

14. 6. 2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2003年 6月12日

出 願 番 号
Application Number: 特願2003-167374
[ST. 10/C]: [JP 2003-167374]

出 願 人
Applicant(s): 松下電器産業株式会社

REC'D 29 JUL 2004

WIPO

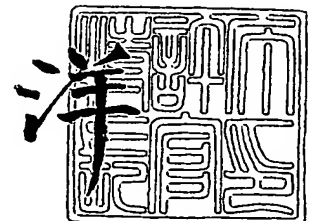
PCT

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 7月14日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願

【整理番号】 2022550095

【提出日】 平成15年 6月12日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 5/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 布田 裕一

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 山道 将人

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 大森 基司

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 館林 誠

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9003742

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号通信システム

【特許請求の範囲】

【請求項 1】 メッセージを秘密に通信する暗号通信システムであって、
1 個のメッセージを記憶している記憶手段と、
前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成する暗号手段と、
前記メッセージに一方向性演算を施して比較演算値を生成する演算手段と、
生成した前記複数の暗号文と前記比較演算値とを送信する送信手段と
を備える暗号送信装置と、
前記複数の暗号文と前記比較演算値とを受信する受信手段と、
前記複数の暗号文の各々に対して、前記暗号化演算に対応する復号演算により同数の復号メッセージを生成する復号手段と、
前記複数の復号メッセージの各々に、前記一方向性演算を施して、同数の復号演算値を生成する演算手段と、
生成した各復号演算値と受信した前記比較演算値とを比較して、少なくとも 1 組の前記復号演算値と前記比較演算値とが一致すれば、前記メッセージの正当な復号文として、当該組に対応する復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力する判定手段と
を備える暗号受信装置と
から構成されることを特徴とする暗号通信システム。

【請求項 2】 前記暗号手段は、NTRU 暗号による暗号化演算により暗号文を生成し、

前記復号手段は、NTRU 暗号による復号演算により復号メッセージを生成する

ことを特徴とする請求項 1 に記載の暗号通信システム。

【請求項 3】 メッセージを秘密に送信する暗号送信装置であって、
1 個のメッセージを記憶している記憶手段と、
前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成

する暗号手段と、

前記メッセージに一方向性演算を施して比較演算値を生成する演算手段と、
生成した前記複数の暗号文と前記比較演算値とを送信する送信手段と
を備えることを特徴とする暗号送信装置。

【請求項 4】 前記暗号手段は、

前記メッセージに対して、可逆のデータ変換を施して、変換メッセージを生成し、生成した変換メッセージに対して、暗号アルゴリズムを施して暗号文を生成する前記暗号化演算を行う暗号化演算部と、

前記暗号化演算部に対して、変換メッセージの生成と暗号文の生成とを前記複数回繰り返すように制御する繰返制御部と

を含むことを特徴とする請求項 3 に記載の暗号送信装置。

【請求項 5】 前記暗号化演算部は、固定長の乱数を生成し、前記メッセージに対して、生成した前記乱数を付加することにより、前記変換メッセージを生成する

ことを特徴とする請求項 4 に記載の暗号送信装置。

【請求項 6】 前記暗号化演算部は、NTRU 暗号による暗号アルゴリズムにより暗号文を生成する

ことを特徴とする請求項 5 に記載の暗号送信装置。

【請求項 7】 暗号送信装置からメッセージを秘密に受信する暗号受信装置であって、

前記暗号送信装置は、1 個のメッセージを記憶しており、前記メッセージに対する複数の暗号化演算により前記同数個の暗号文を生成し、前記メッセージに一方向性演算を施して比較演算値を生成し、生成した前記複数の暗号文と前記比較演算値とを送信し、

前記暗号受信装置は、

前記複数の暗号文と前記比較演算値とを受信する受信手段と、

前記複数の暗号文の各々に対して、前記暗号化演算に対応する復号演算により同数の復号メッセージを生成する復号手段と、

前記複数の復号メッセージの各々に、前記一方向性演算を施して、同数の復号

演算値を生成する演算手段と、

生成した各復号演算値と受信した前記比較演算値とを比較して、少なくとも 1 組の前記復号演算値と前記比較演算値とが一致すれば、前記メッセージの正当な復号文として、当該組に対応する復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力する判定手段とを備えることを特徴とする暗号受信装置。

【請求項 8】 前記暗号送信装置は、前記メッセージに対して、可逆のデータ変換を施して、変換メッセージを生成し、生成した変換メッセージに対して、暗号アルゴリズムを施して暗号文を生成する前記暗号化演算を行い、変換メッセージの生成と暗号文の生成とを前記複数回繰り返す、

前記復号手段は、

前記暗号文に対して、前記暗号アルゴリズムに対応する復号アルゴリズムを施して復号文を生成し、生成した復号文に対して、前記データ変換の逆変換を施して、復号メッセージを生成する前記復号演算を行う復号演算部と、

前記復号演算部とに対して、復号文の生成と復号メッセージの生成とを、前記複数回繰り返すように制御する繰返制御部と

を含むことを特徴とする請求項 7 に記載の暗号受信装置。

【請求項 9】 前記暗号送信装置は、固定長の乱数を生成し、前記メッセージに対して、生成した前記乱数を付加することにより、前記変換メッセージを生成し、

前記復号演算部は、生成した復号文から、前記固定長の乱数部分を除去して復号メッセージを生成する

ことを特徴とする請求項 8 に記載の暗号受信装置。

【請求項 10】 暗号送信装置は、NTRU 暗号による暗号アルゴリズムにより暗号文を生成し、

前記復号演算部は、NTRU 暗号による復号アルゴリズムにより復号文を生成する

ことを特徴とする請求項 9 に記載の暗号受信装置。

【請求項 11】 1 個のメッセージを記憶している記憶手段を備え、前記メッ

セージを秘密に送信する暗号送信装置で用いられる暗号送信方法であって、
前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成する暗号ステップと、
前記メッセージに一方方向性演算を施して比較演算値を生成する演算ステップと、
生成した前記複数の暗号文と前記比較演算値とを送信する送信ステップとを含むことを特徴とする暗号送信方法。

【請求項 12】 1 個のメッセージを記憶している記憶手段を備え、前記メッセージを秘密に送信する暗号送信装置で用いられる暗号送信プログラムであって、
前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成する暗号ステップと、
前記メッセージに一方方向性演算を施して比較演算値を生成する演算ステップと、
生成した前記複数の暗号文と前記比較演算値とを送信する送信ステップとを含むことを特徴とする暗号送信プログラム。

【請求項 13】 コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする請求項 12 に記載の暗号送信プログラム。

【請求項 14】 暗号送信装置からメッセージを秘密に受信する暗号受信装置で用いられる暗号受信方法であって、

前記暗号送信装置は、1 個のメッセージを記憶しており、前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成し、前記メッセージに一方方向性演算を施して比較演算値を生成し、生成した前記複数の暗号文と前記比較演算値とを送信し、

前記暗号受信方法は、
前記複数の暗号文と前記比較演算値とを受信する受信ステップと、
前記複数の暗号文の各々に対して、前記暗号化演算に対応する復号演算により同数の復号メッセージを生成する復号ステップと、
前記複数の復号メッセージの各々に、前記一方方向性演算を施して、同数の復号

演算値を生成する演算ステップと、

生成した各復号演算値と受信した前記比較演算値とを比較して、少なくとも 1 組の前記復号演算値と前記比較演算値とが一致すれば、前記メッセージの正当な復号文として、当該組に対応する復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力する判定ステップと

を含むことを特徴とする暗号受信方法。

【請求項 15】 暗号送信装置からメッセージを秘密に受信する暗号受信装置で用いられる暗号受信プログラムであって、

前記暗号送信装置は、1 個のメッセージを記憶しており、前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成し、前記メッセージに一方方向性演算を施して比較演算値を生成し、生成した前記複数の暗号文と前記比較演算値とを送信し、

前記暗号受信プログラムは、

前記複数の暗号文と前記比較演算値とを受信する受信ステップと、

前記複数の暗号文の各々に対して、前記暗号化演算に対応する復号演算により同数の復号メッセージを生成する復号ステップと、

前記複数の復号メッセージの各々に、前記一方方向性演算を施して、同数の復号演算値を生成する演算ステップと、

生成した各復号演算値と受信した前記比較演算値とを比較して、少なくとも 1 組の前記復号演算値と前記比較演算値とが一致すれば、前記メッセージの正当な復号文として、当該組に対応する復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力する判定ステップと

を含むことを特徴とする暗号受信プログラム。

【請求項 16】 コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする請求項 15 に記載の暗号受信プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報セキュリティ技術としての暗号技術に関する。

【0002】**【従来の技術】**

近年、家庭用電化製品で使用されるような比較的处理能力の低いプロセッサであっても、実装可能なNTRU暗号が注目されている。

NTRU暗号では、多項式演算（加算及び乗算）が基本演算であり、多項式の各係数は、8ビット以下である。このため、8ビットCPUでもNTRU暗号が容易に実装できる。NTRU暗号は、楕円曲線暗号と比較して10～50倍高速であり、また、楕円曲線暗号で必要な多倍長ライブラリが不要であるので、コードサイズが楕円曲線暗号と比較して小さいという利点がある。なお、NTRU暗号については、非特許文献1及び特許文献1により開示されているので、説明を省略する。

【0003】

しかし、NTRU暗号では、復号時にエラーが発生する可能性があり、復号時に、このエラーの検出ができないので、復号が正しく行われたか否かの保証ができないという問題点がある。

この問題点を解決するために、特許文献2によると、送信装置は、平文に一方方向性関数を施して第1関数値を生成し、第1付加情報を生成し、前記平文及び前記第1付加情報に可逆演算を施して、結合情報を生成し、前記結合情報に暗号アルゴリズムを施して暗号文を生成する。受信装置は、第1付加情報と同一の第2付加情報を生成し、前記暗号文に、復号アルゴリズムを施して復号結合情報を生成し、前記復号結合情報及び第2付加情報に前記可逆演算の逆演算を施して、復号文を生成し、復号された復号文に前記一方方向性関数を施して第2関数値を生成し、前記第1関数値と前記第2関数値とを比較し、一致する場合に復号文が正当であると判断する。このようにして、平文が正しく復号できたか否かを判断することができる。

【0004】

平文が正しく復号できなかったと判断される場合には、受信側は、送信側に対

して、再度、暗号文を送信するように要求し、再度暗号文を受信すればよい。

【0005】

【非特許文献1】

Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp. 267-288, Springer-Verlag, 1998

【0006】

【特許文献1】

米国特許番号6,081,597

【0007】

【特許文献2】

特開2002-252611号公報

【0008】

【非特許文献2】

J. Proos, "Imperfect Decryption and an Attack on the NTRU Encryption Scheme", IACR ePrint Archive, 2003/002, <http://eprint.iacr.org/>, (2003).

【0009】

【発明が解決しようとする課題】

しかしながら、非特許文献2によると、NTRU暗号において、攻撃者が受信者に対して適当なデータを送信し、再送要求が起こるか否かをチェックすることにより、鍵を求める攻撃方法が開示されている。このためNTRU暗号を使用する場合において、安全性を確保できないという問題点がある。

【0010】

本発明は、暗号方式において、再送要求による攻撃を回避することができる暗号通信システム、暗号送信装置、暗号送信方法、暗号送信プログラム、暗号受信装置、暗号受信方法及び暗号受信プログラムを提供することを目的とする。

【0011】

【課題を解決するための手段】

上記目的を達成するために、暗号送信装置は、送信する1個のメッセージを5

回暗号化して5個の暗号化メッセージを生成し、メッセージのハッシュ値を算出し、5個の暗号化メッセージとハッシュ値とを送信する。暗号受信装置は、5個の暗号化メッセージとハッシュ値とを受信し、5個の暗号化メッセージを復号してそれぞれ復号メッセージを生成し、生成した復号メッセージの復号ハッシュ値をそれぞれ算出し、算出した復号ハッシュ値と受信したハッシュ値とを比較する。1組でも一致すれば、対応する復号メッセージを正しいものとみなす。5組の全てで一致しなければ、復号エラーとみなす。

【0012】

【発明の実施の形態】

本発明に係る1個の実施の形態としての映像再生システム10について説明する。

1. 映像再生システム10

映像再生システム10は、図1に示すように、サーバ装置100と映像再生装置200とから構成されており、サーバ装置100と映像再生装置200とは、インターネット20を介して接続されている。

【0013】

サーバ装置100は、コンテンツを暗号化し、暗号化コンテンツをインターネット20を介して、映像再生装置200へ送信する。映像再生装置200は、暗号化コンテンツを受信し、受信した暗号化コンテンツを復号してコンテンツを生成し、生成したコンテンツを再生し、映像再生装置200に接続されているモニタ50及びスピーカ40へ映像及び音声を出力する。

【0014】

1. 1 サーバ装置100の構成

サーバ装置100は、図2に示すように、情報記憶部101、乱数生成部102、第1暗号化部103、ハッシュ部104、第2暗号化部105、送受信部106、制御部107、入力部108及び表示部109から構成されている。

サーバ装置100は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニ

ットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、サーバ装置 100 は、その一部の機能を達成する。

【0015】

(1) 情報記憶部 101

情報記憶部 101 は、図 2 に示すように、公開鍵 K_p 、コンテンツ鍵 K_c 及びコンテンツ C を記憶している。

公開鍵 K_p は、NTRU 暗号の鍵生成方法により生成された秘密鍵 K_s (後述する) を元にして生成された公開鍵であり、263 次元の NTRU 暗号の場合に、1841 ビット長である。

【0016】

また、コンテンツ鍵 K_c は、168 ビットの鍵であり、コンテンツ C を暗号化する際に用いられる。

また、コンテンツ C は、映像情報及び音声情報から構成される映画データである。

(2) 乱数生成部 102

乱数生成部 102 は、制御部 107 の制御の基に、64 ビットの乱数 R_i の生成及び生成した乱数 R_i の第 1 暗号化部 103 への出力を、5 回繰り返す。

【0017】

(3) 第 1 暗号化部 103

第 1 暗号化部 103 は、制御部 107 の制御の基に、情報記憶部 101 から公開鍵 K_p 及びコンテンツ鍵 K_c を読み出す。次に、第 1 暗号化部 103 は、制御部 107 の制御の基に、以下の処理 (a) ~ (c) を 5 回繰り返す。

(a) 乱数生成部 102 から乱数 R_i を受け取る。

【0018】

(b) 読み出したコンテンツ鍵 K_c 及び受け取った乱数 R_i を結合する。

$K_c || R_i$

(c) 公開鍵 K_p を用いて、コンテンツ鍵 K_c 及び乱数 R_i の結合に対して、暗号化アルゴリズム $Enc1$ を施して、暗号化コンテンツ鍵 $E K_{ci}$ を生成する

【0019】

$$EKci = Enc1(Kp, Kc || Ri)$$

ここで、「||」は、結合を示す演算子であり、暗号化アルゴリズム $Enc1$ は、NTRU暗号によるアルゴリズムであり、 $X = Enc1(Y, Z)$ は、鍵 Y を用いて、平文 Z に対して暗号化アルゴリズム $Enc1$ を施して暗号文 X を得ることを示す。

【0020】

こうして、5個の暗号化コンテンツ鍵 $EKc1$ 、 $EKc2$ 、 \dots 、 $EKc5$ が生成される。

次に、第1暗号化部103は、生成した5個の暗号化コンテンツ鍵 $EKc1$ 、 $EKc2$ 、 \dots 、 $EKc5$ を送受信部106へ出力する。

なお、図2において、各ブロックは、接続線により他のブロックと接続されている。ただし、一部の接続線を省略している。ここで、各接続線は、信号や情報が伝達される経路を示している。また、第1暗号化部103を示すブロックに接続している複数の接続線のうち、接続線上に鍵マークが付されているものは、第1暗号化部103へ鍵としての情報が伝達される経路を示している。第2暗号化部105を示すブロックについても同様である。また、他の図面についても同様である。

【0021】

(4) ハッシュ部104

ハッシュ部104は、制御部107の制御の基に、情報記憶部101からコンテンツ鍵 Kc を読み出し、読み出したコンテンツ鍵 Kc に対して、一方向性関数であるハッシュ関数 $Hash$ を施して、ハッシュ値 H を生成する。

$$H = Hash(Kc)$$

ここで、ハッシュ関数 $Hash$ の一例は、SHA-1である。なお、SHA-1については、公知であるので、説明を省略する。この場合に、ハッシュ値 H は、160ビット長である。

【0022】

次に、ハッシュ部104は、生成したハッシュ値Hを送受信部106へ出力する。

(5) 第2暗号化部105

第2暗号化部105は、制御部107の制御の基に、情報記憶部101からコンテンツ鍵Kc及びコンテンツCを読み出し、読み出したコンテンツ鍵Kcを用いて、読み出したコンテンツCに暗号化アルゴリズムEnc2を施して、暗号化コンテンツECを生成する。

【0023】

$$EC = Enc2(Kc, C)$$

ここで、暗号化アルゴリズムEnc2は、トリプルDESによるアルゴリズムである。なお、トリプルDESについては、公知であるので、説明を省略する。

次に、第2暗号化部105は、生成した暗号化コンテンツECを送受信部106へ出力する。

【0024】

(6) 送受信部106

送受信部106は、インターネット20を介して、映像再生装置200と接続されている。

送受信部106は、制御部107の制御の基に、第1暗号化部103から5個の暗号化コンテンツ鍵EKc1、EKc2、・・・、EKc5を受け取り、ハッシュ部104からハッシュ値Hを受け取り、第2暗号化部105から暗号化コンテンツECを受け取り、受け取った5個の暗号化コンテンツ鍵EKc1、EKc2、・・・、EKc5、ハッシュ値H及び暗号化コンテンツECを、インターネット20を介して、映像再生装置200へ送信する。

【0025】

(7) 制御部107、入力部108及び表示部109

制御部107は、乱数生成部102、第1暗号化部103、ハッシュ部104、第2暗号化部105及び送受信部106を制御する。

入力部108は、サーバ装置100の操作者から操作指示を受け付け、受け付けた指示を制御部107へ出力する。

【0026】

表示部109は、制御部107の制御の基に、各種の情報を表示する。

1. 2 映像再生装置200の構成

映像再生装置200は、図3に示すように、送受信部201、第1復号部202、ハッシュ部203、判定部204、情報記憶部205、第2復号部206、再生部207、制御部208、入力部209及び表示部210から構成されている。

【0027】

映像再生装置200は、サーバ装置100と同様に、マイクロプロセッサ、ROM、RAMなどを含んで構成される。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、映像再生装置200は、その一部の機能を達成する。

【0028】

(1) 情報記憶部205

情報記憶部205は、図3に示すように、秘密鍵 K_s を記憶している。

秘密鍵 K_s は、NTRU暗号の鍵生成方法により生成された秘密鍵であり、263次元のNTRU暗号の場合には、415ビット長である。

(2) 送受信部201

送受信部201は、インターネット20を介して、サーバ装置100と接続されている。

【0029】

送受信部201は、制御部208の制御の基に、インターネット20を介して、サーバ装置100から、5個の暗号化コンテンツ鍵 EK_{c1} 、 EK_{c2} 、 \dots 、 EK_{c5} 、ハッシュ値 H 及び暗号化コンテンツ EC を受け取り、受け取った5個の暗号化コンテンツ鍵 EK_{c1} 、 EK_{c2} 、 \dots 、 EK_{c5} を第1復号部202へ出力し、受け取ったハッシュ値 H を判定部204へ出力し、受け取った暗号化コンテンツ EC を第2復号部206へ出力する。

【0030】

(3) 第1復号部202

第1復号部202は、制御部208の制御の基に、送受信部201から5個の暗号化コンテンツ鍵 $EKc1$ 、 $EKc2$ 、 \dots 、 $EKc5$ を受け取り、情報記憶部205から秘密鍵 Ks を読み出す。次に、第1復号部202は、制御部208の制御の基に、以下の処理(a)～(c)を5回繰り返す。

【0031】

(a) 秘密鍵 Ks を用いて、暗号化コンテンツ鍵 $EKci$ に対して、復号アルゴリズム $Dec1$ を施して、コンテンツ鍵 $DKci$ を生成する。

$$DKci = Dec1(Ks, EKci)$$

ここで、復号アルゴリズム $Dec1$ は、NTRU暗号によるアルゴリズムであり、暗号化アルゴリズム $Enc1$ により生成された暗号文を復号する。 $Z = Dec1(Y, X)$ は、鍵 Y を用いて、暗号文 X に対して復号アルゴリズム $Dec1$ を施して復号文 Z を得ることを示す。

【0032】

(b) 次に、生成したコンテンツ鍵 $DKci$ のうち、末尾の64ビットの乱数部分を削除する。

(c) 乱数部分が削除されたコンテンツ鍵 $DKci$ をハッシュ部203及び判定部204へ出力する。

こうして、5個のコンテンツ鍵 $DKci$ が、ハッシュ部203及び判定部204へ出力される。

【0033】

(4) ハッシュ部203

ハッシュ部203は、制御部208の制御の基に、以下の処理(a)～(b)を5回繰り返す。

(a) 第1復号部202からコンテンツ鍵 $DKci$ を受け取る。

(b) 受け取ったコンテンツ鍵 $DKci$ に対して、ハッシュ関数 $Hash$ を施して、ハッシュ値 Hi を生成する。

【0034】

$$Hi = Hash(DKci)$$

次に、ハッシュ部 203 は、生成したハッシュ値 H_i を判定部 204 へ出力する。

(5) 判定部 204

判定部 204 は、制御部 208 の制御の基に、送受信部 201 からハッシュ値 H を受け取り、以下の処理 (a) ~ (d) を 5 回繰り返す。

【0035】

- (a) ハッシュ部 203 からハッシュ値 H_i を受け取る。
- (b) 第 1 復号部 202 からコンテンツ鍵 DK_{ci} を受け取る。
- (c) ハッシュ値 H とハッシュ値 H_i とが一致しているか否かを判定する。
- (d) 一致している場合に、 i の値とコンテンツ鍵 DK_{ci} とを対応付けて記憶する。

【0036】

上記の処理 (a) ~ (b) の 5 回の繰り返しが終了した後、記憶している i の値があれば、暗号化コンテンツ鍵の復号が正しく行われたものと判断し、 i の値と対応付けて記憶しているコンテンツ鍵 DK_{ci} を第 2 復号部 206 へ出力し、復号が正しく行われたことを示す復号結果を制御部 208 へ出力する。

記憶している i の値がなければ、暗号化コンテンツ鍵の復号が正しく行われなかったものと判断し、その旨を示す復号結果を制御部 208 へ出力する。

【0037】

(6) 第 2 復号部 206

第 2 復号部 206 は、制御部 208 の制御の基に、判定部 204 からコンテンツ鍵 DK_{ci} を受け取り、送受信部 201 から暗号化コンテンツ EC を受け取り、受け取ったコンテンツ鍵 DK_{ci} を用いて、受け取った暗号化コンテンツ EC に復号アルゴリズム Dec_2 を施して、コンテンツ C を生成する。

【0038】

ここで、復号アルゴリズム Dec_2 は、トリプル DES によるアルゴリズムであり、暗号化アルゴリズム Enc_2 により生成された暗号文を復号する。

次に、第 2 復号部 206 は、生成したコンテンツ C を再生部 207 へ出力する。

(7) 再生部 207

再生部 207 は、制御部 208 の制御の基に、第 2 復号部 206 からコンテンツ C を受け取り、受け取ったコンテンツ C を再生して、映像信号と音声信号とを生成し、生成した映像信号と音声信号とをそれぞれ、モニタ 50 及びスピーカ 40 へ出力する。

【0039】

モニタ 50 及びスピーカ 40 は、それぞれ映像と音声とを出力する。

(8) 制御部 208、入力部 209 及び表示部 210

制御部 208 は、送受信部 201、第 1 復号部 202、ハッシュ部 203、判定部 204、第 2 復号部 206 及び再生部 207 を制御する。

制御部 208 は、判定部 204 から、暗号化コンテンツ鍵の復号が正しく行われた旨及び正しく行われなかった旨をそれぞれ示す復号結果を受け取る。

【0040】

正しく行われなかった旨を示す復号結果を受け取ると、第 2 復号部 206 に対して復号を行わないように制御し、表示部 210 に対して、復号エラーを表示するように制御する。

正しく行われた旨を示す復号結果を受け取ると、第 2 復号部 206 に対して復号を行うように制御する。

【0041】

入力部 209 は、映像再生装置 200 の利用者から操作指示を受け付け、受け付けた指示を制御部 208 へ出力する。

表示部 210 は、制御部 208 の制御の基に、各種の情報を表示する。

1. 3 映像再生システム 10 の動作

映像再生システム 10 の動作について説明する。

【0042】

(1) サーバ装置 100 の動作

サーバ装置 100 の動作について、図 4 に示すフローチャートを用いて説明する。

第 1 暗号化部 103 は、情報記憶部 101 からコンテンツ鍵 Kc を読み出し

(ステップS101)、次に、公開鍵 K_p を読み出す(ステップS102)。

【0043】

次に、制御部107は、ステップS103～S106において、ステップS104～S105を5回繰り返すように制御する。なお、以下に記載の乱数 R_i 及び暗号化コンテンツ鍵 EK_{ci} の表記における「 i 」は、繰り返しの各回を示すサフィクスであり、繰り返しにおいて、 $i=1, 2, 3, 4, 5$ のように変化するものである。

【0044】

乱数生成部102は、64ビットの乱数 R_i を生成し、生成した乱数 R_i を第1暗号化部103へ出力し(ステップS104)、第1暗号化部103は、コンテンツ鍵 K_c 及び乱数 R_i を結合し、公開鍵 K_p を用いて、コンテンツ鍵 K_c 及び乱数 R_i の結合に対して、暗号化アルゴリズム $Enc1$ を施して、暗号化コンテンツ鍵 EK_{ci} を生成する(ステップS105)。

【0045】

このようにしてステップS104からステップS105までが5回繰り返されることにより、5個の暗号化コンテンツ鍵 $EK_{c1}, EK_{c2}, \dots, EK_{c5}$ が生成される。

次に、ハッシュ部104は、情報記憶部101からコンテンツ鍵 K_c を読み出し、読み出したコンテンツ鍵 K_c に対して、一方向性関数であるハッシュ関数 $Hash$ を施して、ハッシュ値 H を生成する(ステップS107)。

【0046】

次に、第2暗号化部105は、情報記憶部101からコンテンツ鍵 K_c を読み出し(ステップS108)、コンテンツ C を読み出し(ステップS109)、読み出したコンテンツ鍵 K_c を用いて、読み出したコンテンツ C に暗号化アルゴリズム $Enc2$ を施して、暗号化コンテンツ EC を生成する(ステップS110)。

【0047】

次に、送受信部106は、5個の暗号化コンテンツ鍵 $EK_{c1}, EK_{c2}, \dots, EK_{c5}$ 、ハッシュ値 H 及び暗号化コンテンツ EC を、インターネット2

0を介して、映像再生装置200へ送信する(ステップS111)。

(2) 映像再生装置200の動作

映像再生装置200の動作について、図5～図6に示すフローチャートを用いて説明する。

【0048】

送受信部201は、インターネット20を介して、サーバ装置100から、5個の暗号化コンテンツ鍵EKc1、EKc2、・・・、EKc5、ハッシュ値H及び暗号化コンテンツECを受け取り、受け取った5個の暗号化コンテンツ鍵EKc1、EKc2、・・・、EKc5を第1復号部202へ出力し、受け取ったハッシュ値Hを判定部204へ出力し、受け取った暗号化コンテンツECを第2復号部206へ出力する(ステップS131)。

【0049】

第1復号部202は、情報記憶部205から秘密鍵Ksを読み出す(ステップS132)。次に、制御部208は、ステップS133～S139において、ステップS134～S138を5回繰り返すように制御する。なお、以下の暗号化コンテンツ鍵EKci、コンテンツ鍵DKci及びハッシュ値Hiの表記における「i」は、繰り返しの各回を示すサフィクスであり、繰り返しにおいて、i=1、2、3、4、5のように変化するものである。

【0050】

第1復号部202は、秘密鍵Ksを用いて、暗号化コンテンツ鍵EKciに対して、復号アルゴリズムDec1を施して、コンテンツ鍵DKciを生成し(ステップS134)、次に、生成したコンテンツ鍵DKciのうち、末尾の64ビットの乱数部分を削除し、乱数部分が削除されたコンテンツ鍵DKciをハッシュ部203及び判定部204へ出力する(ステップS135)。

【0051】

次に、ハッシュ部203は、第1復号部202からコンテンツ鍵DKciを受け取り、受け取ったコンテンツ鍵DKciに対して、ハッシュ関数Hashを施して、ハッシュ値Hiを生成する(ステップS136)。

次に、判定部204は、ハッシュ部203からハッシュ値Hiを受け取り、第

1 復号部 202 からコンテンツ鍵 $DK_c i$ を受け取り、ハッシュ値 H とハッシュ値 H_i とが一致しているか否かを判定し (ステップ S137)、一致している場合に (ステップ S137)、このときの i の値とコンテンツ鍵 $DK_c i$ とを対応付けて記憶する (ステップ S138)。

【0052】

ステップ S134～S138 が 5 回繰り返しの後で、記憶している i の値があれば (ステップ S140)、暗号化コンテンツ鍵の復号が正しく行われたものと判断し、第 2 復号部 206 は、判定部 204 からコンテンツ鍵 $DK_c i$ を受け取り、送受信部 201 から暗号化コンテンツ EC を受け取り、受け取ったコンテンツ鍵 $DK_c i$ を用いて、受け取った暗号化コンテンツ EC に復号アルゴリズム Dec_2 を施して、コンテンツ C を生成し (ステップ S141)、再生部 207 は、第 2 復号部 206 からコンテンツ C を受け取り、受け取ったコンテンツ C を再生して、映像信号と音声信号とを生成し、生成した映像信号と音声信号とをそれぞれ、モニタ 50 及びスピーカ 40 へ出力し、モニタ 50 及びスピーカ 40 は、それぞれ映像と音声とを出力する (ステップ S142)。

【0053】

記憶している i の値がなければ (ステップ S140)、判定部 204 は、5 個の暗号化コンテンツ鍵の復号が全て正しく行われなかったものと判断し、その旨を示す復号結果を制御部 208 へ出力し、制御部 208 は、第 2 復号部 206 に対して復号を行わないように制御し、表示部 210 に対して、復号エラーを表示するように制御し、表示部 210 は、復号エラーを表示する (ステップ S143)。

【0054】

なお、上記において、制御部 208 は、ステップ S133～S139 において、ステップ S134～S138 を 5 回繰り返すように制御するとしているが、ステップ S137 において、ハッシュ値 H とハッシュ値 H_i とが一致していると判定された場合に、ステップ S134～S138 のループを抜けるとしてもよい。

1. 4 まとめ

以上説明したように、上記の実施の形態では、メッセージ m (実施の形態では

、コンテンツ鍵)を複数回暗号化して送信することにより、メッセージ m が復元不可能となる確率を小さくするようにしている。こうして、メッセージ m の再送要求の発生確率が小さくなる。

【0055】

送信装置(実施の形態では、サーバ装置)は、乱数 $R_1 \sim R_5$ を生成し、 $m \parallel R_1$ 、 $m \parallel R_2$ 、 $m \parallel R_3$ 、 $m \parallel R_4$ 及び $m \parallel R_5$ を生成し、それぞれを暗号化して $Enc(m \parallel R_1)$ 、 $Enc(m \parallel R_2)$ 、 $Enc(m \parallel R_3)$ 、 $Enc(m \parallel R_4)$ 及び $Enc(m \parallel R_5)$ を生成する。ここで、 $Enc(X)$ は、平文 X に暗号化アルゴリズム Enc を施して暗号文を生成することを示している。次に、ハッシュ値 $H(m)$ を計算する。次に、 $Enc(m \parallel R_1)$ 、 $Enc(m \parallel R_2)$ 、 $Enc(m \parallel R_3)$ 、 $Enc(m \parallel R_4)$ 、 $Enc(m \parallel R_5)$ 及びハッシュ値 $H(m)$ を受信装置(実施の形態では、映像再生装置)へ送信する。

【0056】

受信装置は、 $Enc(m \parallel R_1)$ 、 $Enc(m \parallel R_2)$ 、 $Enc(m \parallel R_3)$ 、 $Enc(m \parallel R_4)$ 、 $Enc(m \parallel R_5)$ 及びハッシュ値 $H(m)$ を受信し、 $Enc(m \parallel R_1)$ 、 $Enc(m \parallel R_2)$ 、 $Enc(m \parallel R_3)$ 、 $Enc(m \parallel R_4)$ 、 $Enc(m \parallel R_5)$ を復号して、メッセージに相当する部分 m_1 、 \dots 、 m_5 を取得する。さらに、 m_1 、 \dots 、 m_5 のハッシュ値 $H(m_1)$ 、 \dots 、 $H(m_5)$ を計算し、それぞれ計算したハッシュ値と受信したハッシュ値 $H(m)$ とを比較する。この比較において、計算したハッシュ値と受信したハッシュ値 $H(m)$ とが一致するものが、1組でも存在するならば、一致するハッシュ値に対応するメッセージ(m_1 、 \dots 、 m_5 のいずれか)を復号文として出力する。ハッシュ値が一致するものが全く存在しなければ、復号エラーを示す $False$ を出力する。

【0057】

263次元のNTRU暗号において、暗号文の1つ1つが復号エラーを起こす確率は、 10^{-5} 程度である。上記の実施の形態では、5個の暗号文を送信するので、再生要求が発生する確率は、 10^{-25} ($= 10^{-5} \times 10^{-5} \times 10^{-5} \times 10^{-5}$

$\times 10^{-5}$) 程度となる。一方、1024ビットのRSA暗号の場合における攻撃成功確率は、 $2^{-80} = 10^{-24}$ である。このため、263次元のNTRU暗号において、上記の実施の形態を適用した場合には、1024ビットのRSA暗号の場合における攻撃成功確率を下回ることとなる。

【0058】

2. その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

(1) 上記の実施の形態では、コンテンツ鍵を暗号化して生成した暗号化コンテンツ鍵を5個送信するとしているが、コンテンツを暗号化して生成した暗号化コンテンツを5個送信するとしてもよい。

【0059】

(2) 上記の実施の形態では、送信装置は、5個の暗号文を生成して送信し、受信装置は、5個の暗号文を受信して復号するとしているが、暗号文の生成個数が5個に限定されることはない。例えば、3個でもよいし、7個でもよい。送信装置は、2個以上の暗号文を生成して送信し、受信装置は、これらの暗号文を受信して復号し、これらの結果により、復号時のエラーの判定を行うとしてもよい。上述したように、暗号文の個数は、攻撃成功確率に影響し、暗号文の個数が多ければ多いほど、攻撃成功確率は、低くなる。

【0060】

(3) 上記の実施の形態では、暗号化されるメッセージ m とその都度生成した乱数との結合体に対して暗号化アルゴリズムを施すとしているが、送信装置は、メッセージ m に対してさらに他の演算を施して、演算結果と乱数との結合体に対して暗号化アルゴリズムを施すとしてもよい。

例えば、送信装置は、メッセージ m に、「0」、「1」、「2」、「3」及び「4」をそれぞれ加算して「 m 」、「 $m+1$ 」、「 $m+2$ 」、「 $m+3$ 」及び「 $m+4$ 」を算出し、それぞれの算出結果と乱数との結合体に対して暗号化アルゴリズムを施して、

$Enc(m || R1)$ 、 $Enc(m+1 || R2)$ 、 $Enc(m+2 || R3)$ 、 $Enc(m+3 || R4)$ 、 $Enc(m+4 || R5)$ を生成する。

【0061】

受信装置は、 $Enc(m || R1)$ 、 $Enc(m+1 || R2)$ 、 $Enc(m+2 || R3)$ 、 $Enc(m+3 || R4)$ 、 $Enc(m+4 || R5)$ を復号し、それぞれの復号結果から、末尾の所定長の乱数部分を削除し、乱数部分が削除された復号結果から、「0」、「1」、「2」、「3」及び「4」をそれぞれ減じてメッセージ m に相当する情報を得る。

【0062】

(4) 上記の実施の形態では、送信装置は、メッセージ m と乱数とをこの順序で結合し、結合結果に対して暗号化アルゴリズムを施すとしているが、結合の順序を逆にしてもよい。つまり、乱数とメッセージ m とをこの順序で結合するとしてもよい。また、メッセージ m と乱数とを1ビットずつ交互に結合してもよい。このとき、受信装置は、それぞれ逆の演算を行うことにより、メッセージ m に相当する情報を得ることができる。

【0063】

(5) 上記の実施の形態では、サーバ装置は、インターネットを介して、5個の暗号化コンテンツ鍵、暗号化コンテンツ及びハッシュ値を、映像再生装置へ送信するとしているが、この実施の形態に限定されることはない。

サーバ装置に代えてデジタル放送送信装置により、5個の暗号化コンテンツ鍵、暗号化コンテンツ及びハッシュ値を、インターネットに代えてデジタル放送波に載せて放送し、映像再生装置に代えてデジタル放送受信装置は、デジタル放送波を受信し、受信したデジタル放送波から5個の暗号化コンテンツ鍵、暗号化コンテンツ及びハッシュ値を抽出するとしてもよい。

【0064】

(6) 映像再生システム 10 は、映像再生装置 200 に代えて、図7に示す映像再生装置 200b 及びメモリカード 300b を含むとしてもよい。

映像再生装置 200b は、映像再生装置 200 の一部の機能を備え、メモリカード 300b は、映像再生装置 200 の他の一部の機能を備える。

つまり、メモ리카ード300bは、利用者により映像再生装置200bに装着され、映像再生装置200bを介して、サーバ装置100から、5個の暗号化コンテンツ鍵とハッシュ値とを受け取り、各暗号化コンテンツ鍵が正しく復号されるか否かを判定し、正しく復号されると判定する場合に、正しく復号されたコンテンツ鍵を映像再生装置200bへ出力する。映像再生装置200bは、メモ리카ード300bからコンテンツ鍵を受け取り、サーバ装置100から受け取った暗号化コンテンツを復号して再生する。

【0065】

具体的には、映像再生装置200bは、図7に示すように、送受信部201、第2復号部206、再生部207、制御部208、入力部209、表示部210、入出力部211及び認証部212から構成されている。

ここで、映像再生装置200bの構成要素である送受信部201、第2復号部206、再生部207、制御部208、入力部209及び表示部210は、それぞれ、映像再生装置200の構成要素である送受信部201、第2復号部206、再生部207、制御部208、入力部209及び表示部210と同様のものである。また、入出力部211は、メモ리카ード300bと映像再生装置200bの他の構成要素との間で情報の入出力を行う。さらに、認証部212は、何らかのメモ리카ードが映像再生装置200bに装着されたときに、装着されたメモ리카ードとの間で、相互の機器認証を行う。機器認証が成功した場合に限り、その後の入出力が行われる。

【0066】

また、メモ리카ード300bは、図7に示すように、入出力部301、認証部302、第1復号部202b、ハッシュ部203b、判定部204b、情報記憶部205bから構成されている。

ここで、第1復号部202b、ハッシュ部203b、判定部204b及び情報記憶部205bは、それぞれ、映像再生装置200の構成要素である第1復号部202、ハッシュ部203、判定部204及び情報記憶部205と同様のものである。また、入出力部301は、メモ리카ード300bの他の構成要素と映像再生装置200bとの間で情報の入出力を行う。さらに、認証部302は、メモリ

カード 300b が何らかの装置に装着されたときに、装着された装置との間で、相互の機器認証を行う。機器認証が成功した場合に限り、その後の入出力が行われる。

【0067】

(7) 別の実施の形態

本発明に係る別の実施の形態としての BD 再生システム 10c について説明する。

BD 再生システム 10c は、図 8 に示すように、サーバ装置 100c、BD プレイヤ 200c 及び携帯電話 400c から構成されており、サーバ装置 100c と携帯電話 400c とは、インターネット 20、携帯電話網 25 及び無線基地局 26 を介して、接続されている。

【0068】

(BD 再生システム 10c の構成)

サーバ装置 100c は、サーバ装置 100 と同様の構成を有している。

BD プレイヤ 200c は、図 9 に示すように、ドライブ部 213、第 2 復号部 206、再生部 207、制御部 208、入力部 209、表示部 210、入出力部 211 及び認証部 212 から構成されている。

【0069】

ここで、BD プレイヤ 200c の構成要素である第 2 復号部 206、再生部 207、制御部 208、入力部 209 及び表示部 210 は、それぞれ、映像再生装置 200 の構成要素である第 2 復号部 206、再生部 207、制御部 208、入力部 209 及び表示部 210 と同様のものである。また、入出力部 211 は、メモリカード 300c と BD プレイヤ 200c の他の構成要素との間で情報の入出力を行う。さらに、認証部 212 は、何らかのメモリカードが BD プレイヤ 200c に装着されたときに、装着されたメモリカードとの間で、相互の機器認証を行う。機器認証が成功した場合に限り、その後の入出力が行われる。ドライブ部 213 は、装着された BD 60 から暗号化コンテンツを読み出し、読み出した暗号化コンテンツを第 2 復号部 206 へ出力する。

【0070】

また、メモリカード 300c は、図 9 に示すように、入出力部 301c、認証部 302c、第 1 復号部 202c、ハッシュ部 203c、判定部 204c、情報記憶部 205c から構成されている。

ここで、第 1 復号部 202c、ハッシュ部 203c、判定部 204c 及び情報記憶部 205c は、それぞれ、映像再生装置 200 の構成要素である第 1 復号部 202、ハッシュ部 203、判定部 204 及び情報記憶部 205 と同様のものである。また、入出力部 301c は、メモリカード 300c の他の構成要素と BD プレイヤ 200c との間で情報の入出力を行う。さらに、認証部 302c は、メモリカード 300c が何らかの装置に装着されたときに、装着された装置との間で、相互の機器認証を行う。機器認証が成功した場合に限り、その後の入出力が行われる。情報記憶部 205 は、秘密鍵 K_s 、5 個の暗号化コンテンツ鍵、ハッシュ値及び再生されたコンテンツ鍵を記憶するための領域を備えている。

【0071】

(BD 再生システム 10c の動作)

コンテンツ鍵を用いてコンテンツを暗号化して生成された暗号化コンテンツを記録している BD 60 が配布され、利用者は、配布された BD 60 を入手する。

コンテンツ鍵は、次に示すように、BD 60 の配布とは異なる別のルートを紹介して配布される。

【0072】

サーバ装置 100c は、サーバ装置 100 と同様に、コンテンツ鍵から 5 個の暗号化コンテンツ鍵とハッシュ値とを生成し、生成した 5 個の暗号化コンテンツ鍵とハッシュ値とを、インターネット 20、携帯電話網 25 及び無線基地局 26 を介して、携帯電話 400c へ送信する。

携帯電話 400c には、利用者によりメモリカード 300c が装着される。

【0073】

携帯電話 400c は、サーバ装置 100c から 5 個の暗号化コンテンツ鍵とハッシュ値とを受信し、受信した 5 個の暗号化コンテンツ鍵とハッシュ値とをメモリカード 300c の入出力部 301c を介して、情報記憶部 205c へ書き込む。

メモ리카ード300cの情報記憶部205cは、5個の暗号化コンテンツ鍵とハッシュ値とを一旦記憶し、第1復号部202cは、情報記憶部205cから各暗号化コンテンツ鍵を読み出して復号し、復号結果のコンテンツ鍵をハッシュ部203c及び判定部204cへ出力する。判定部204cは、情報記憶部205cからハッシュ値を読み出し、読み出したハッシュ値と、第1復号部202cから受け取った復号結果のコンテンツ鍵とを用いて、各暗号化コンテンツ鍵が正しく復号されるか否かを判定し、正しく復号されると判定する場合に、正しく復号されたコンテンツ鍵を情報記憶部205cに書き込む。

【0074】

メモ리카ード300c及びBD60は、利用者により、BDプレイヤー200cに装着される。

BDプレイヤー200cは、BD60から暗号化コンテンツを読み出し、メモ리카ード300cの情報記憶部205cから正しく復号されたコンテンツ鍵を読み出し、読み出したコンテンツ鍵を用いて、読み出した暗号化コンテンツを復号してコンテンツを生成し、生成したコンテンツを再生し、BDプレイヤー200cに接続されているモニタ50及びスピーカ40へ映像及び音声を出力する。

【0075】

(8) 上記の実施の形態において、263次元のNTRU暗号方式を用いるとし、秘密鍵及び公開鍵のビット長は、それぞれ、415ビット、1841ビットであるとしているが、これらの次元やビット数には限定されない。

また、ハッシュ部104及びハッシュ部203は、ハッシュ関数Hashとして、SHA-1を用いるとしているが、他のハッシュ関数を用いるとしてもよい。

【0076】

(9) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディス

ク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0077】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0078】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(10) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0079】

【発明の効果】

以上説明したように、本発明は、メッセージを秘密に通信する暗号通信システムであって、1個のメッセージを記憶している記憶手段と、前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成する暗号手段と、前記メッセージに一方向性演算を施して比較演算値を生成する演算手段と、生成した前記複数の暗号文と前記比較演算値とを送信する送信手段とを備える暗号送信装置と、前記複数の暗号文と前記比較演算値とを受信する受信手段と、前記複数の暗号文の各々に対して、前記暗号化演算に対応する復号演算により同数の復号メッセージを生成する復号手段と、前記複数の復号メッセージの各々に、前記一方

向性演算を施して、同数の復号演算値を生成する演算手段と、生成した各復号演算値と受信した前記比較演算値とを比較して、少なくとも1組の前記復号演算値と前記比較演算値とが一致すれば、前記メッセージの正当な復号文として、当該組に対応する復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力する判定手段とを備える暗号受信装置とから構成される。また、メッセージを秘密に送信する暗号送信装置であって、1個のメッセージを記憶している記憶手段と、前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成する暗号手段と、前記メッセージに一方向性演算を施して比較演算値を生成する演算手段と、生成した前記複数の暗号文と前記比較演算値とを送信する送信手段とを備える。また、暗号送信装置からメッセージを秘密に受信する暗号受信装置であって、前記暗号送信装置は、1個のメッセージを記憶しており、前記メッセージに対する複数回の暗号化演算により前記同数個の暗号文を生成し、前記メッセージに一方向性演算を施して比較演算値を生成し、生成した前記複数の暗号文と前記比較演算値とを送信し、前記暗号受信装置は、前記複数の暗号文と前記比較演算値とを受信する受信手段と、前記複数の暗号文の各々に対して、前記暗号化演算に対応する復号演算により同数の復号メッセージを生成する復号手段と、前記複数の復号メッセージの各々に、前記一方向性演算を施して、同数の復号演算値を生成する演算手段と、生成した各復号演算値と受信した前記比較演算値とを比較して、少なくとも1組の前記復号演算値と前記比較演算値とが一致すれば、前記メッセージの正当な復号文として、当該組に対応する復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力する判定手段とを備える。

【0080】

これらの構成によると、暗号送信装置は、メッセージから複数個の暗号文を生成し、前記メッセージに一方向性演算を施して比較演算値を生成し、暗号受信装置は、前記複数の暗号文を復号して同数の復号メッセージを生成し、前記複数の復号メッセージに、前記一方向性演算を施して、同数の復号演算値を生成し、少なくとも1組の前記復号演算値と前記比較演算値とが一致すれば、当該組に対応

する正当な復号メッセージを出力し、全ての組の前記復号演算値と前記比較演算値とが不一致であれば、復号エラーを出力するので、復号時にエラーが発生する確率を低く抑え、再送要求による攻撃を回避できる可能性を高くすることができる。

【0081】

ここで、前記暗号手段は、前記メッセージに対して、可逆のデータ変換を施して、変換メッセージを生成し、生成した変換メッセージに対して、暗号アルゴリズムを施して暗号文を生成する前記暗号化演算を行う暗号化演算部と、前記暗号化演算部に対して、変換メッセージの生成と暗号文の生成とを前記複数回繰り返すように制御する繰返制御部とを含む。また、前記暗号送信装置は、前記メッセージに対して、可逆のデータ変換を施して、変換メッセージを生成し、生成した変換メッセージに対して、暗号アルゴリズムを施して暗号文を生成する前記暗号化演算を行い、変換メッセージの生成と暗号文の生成とを前記複数回繰り返す、前記復号手段は、前記暗号文に対して、前記暗号アルゴリズムに対応する復号アルゴリズムを施して復号文を生成し、生成した復号文に対して、前記データ変換の逆変換を施して、復号メッセージを生成する前記復号演算を行う復号演算部と、前記復号演算部とに対して、復号文の生成と復号メッセージの生成とを、前記複数回繰り返すように制御する繰返制御部とを含む。

【0082】

これらの構成によると、暗号送信装置は、メッセージに対して、可逆のデータ変換を施して生成した変換メッセージに対して、暗号アルゴリズムを施して暗号文を生成するので、送信される暗号文が送信路で盗聴され、解読された場合であっても、元のメッセージの復号が容易に知られないようにすることができる。また、暗号受信装置は、前記暗号文に対して、前記暗号アルゴリズムに対応する復号アルゴリズムを施して生成した復号文に対して、前記データ変換の逆変換を施して、復号メッセージを生成するので、メッセージに相当する復号メッセージを確実に得ることができる。

【0083】

ここで、前記暗号化演算部は、固定長の乱数を生成し、前記メッセージに対し

て、生成した前記乱数を付加することにより、前記変換メッセージを生成する。
また、前記暗号送信装置は、固定長の乱数を生成し、前記メッセージに対して、生成した前記乱数を付加することにより、前記変換メッセージを生成し、前記復号演算部は、生成した復号文から、前記固定長の乱数部分を除去して復号メッセージを生成する。

【0084】

これらの構成によると、暗号送信装置は、前記メッセージに対して、固定長の乱数を付加して変換メッセージを生成するので、逆変換が容易である。また、暗号受信装置は、生成した復号文から、前記固定長の乱数部分を除去して復号メッセージを生成するので、メッセージに相当する復号メッセージを確実に得ることができる。

【図面の簡単な説明】

【図1】

本発明に係る1個の実施の形態としての映像再生システム10の構成を示すシステム構成図である。

【図2】

サーバ装置100の構成を示す機能ブロック図である。

【図3】

映像再生装置200の構成を示す機能ブロック図である。

【図4】

サーバ装置100の動作を示すフローチャートである。

【図5】

映像再生装置200の動作を示すフローチャートである。図6へ続く。

【図6】

映像再生装置200の動作を示すフローチャートである。図5から続く。

【図7】

変形例としての映像再生システム10に含まれる映像再生装置200b及びメモリカード300bの構成を示す機能ブロック図である。

【図8】

本発明に係る別の実施の形態としてのBD再生システム10cの構成を示すシステム構成図である。

【図9】

BD再生システム10cに含まれるメモリカード300c及びBDプレイヤー200cの構成を示す機能ブロック図である。

【符号の説明】

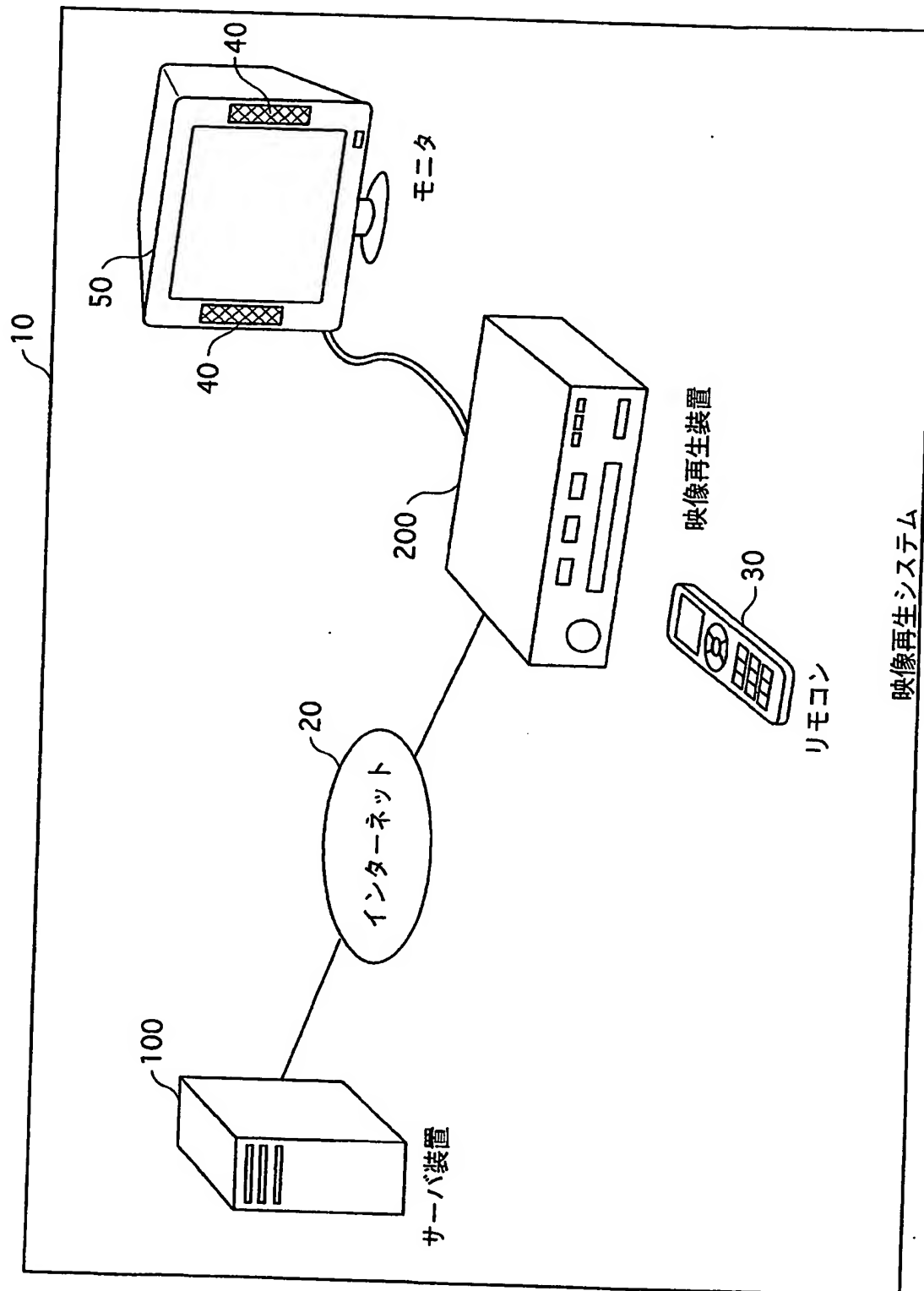
- 10 映像再生システム
- 10c BD再生システム
- 20 インターネット
- 25 携帯電話網
- 26 無線基地局
- 40 スピーカ
- 50 モニタ
- 60 BD
- 100、100c サーバ装置
- 101 情報記憶部
- 102 乱数生成部
- 103 第1暗号化部
- 104 ハッシュ部
- 105 第2暗号化部
- 106 送受信部
- 107 制御部
- 108 入力部
- 109 表示部
- 200、200b 映像再生装置
- 200c BDプレイヤー
- 201 送受信部
- 202、202b、202c 第1復号部
- 203、203b、203c ハッシュ部

2 0 4、2 0 4 b、2 0 4 c 判定部
2 0 5、2 0 5 b、2 0 5 c 情報記憶部
2 0 6 第 2 復号部
2 0 7 再生部
2 0 8 制御部
2 0 9 入力部
2 1 0 表示部
2 1 1 入出力部
2 1 2 認証部
2 1 3 ドライブ部
3 0 0 b、3 0 0 c メモリカード
3 0 1、3 0 1 c 入出力部
3 0 2、3 0 2 c 認証部
4 0 0 c 携帯電話

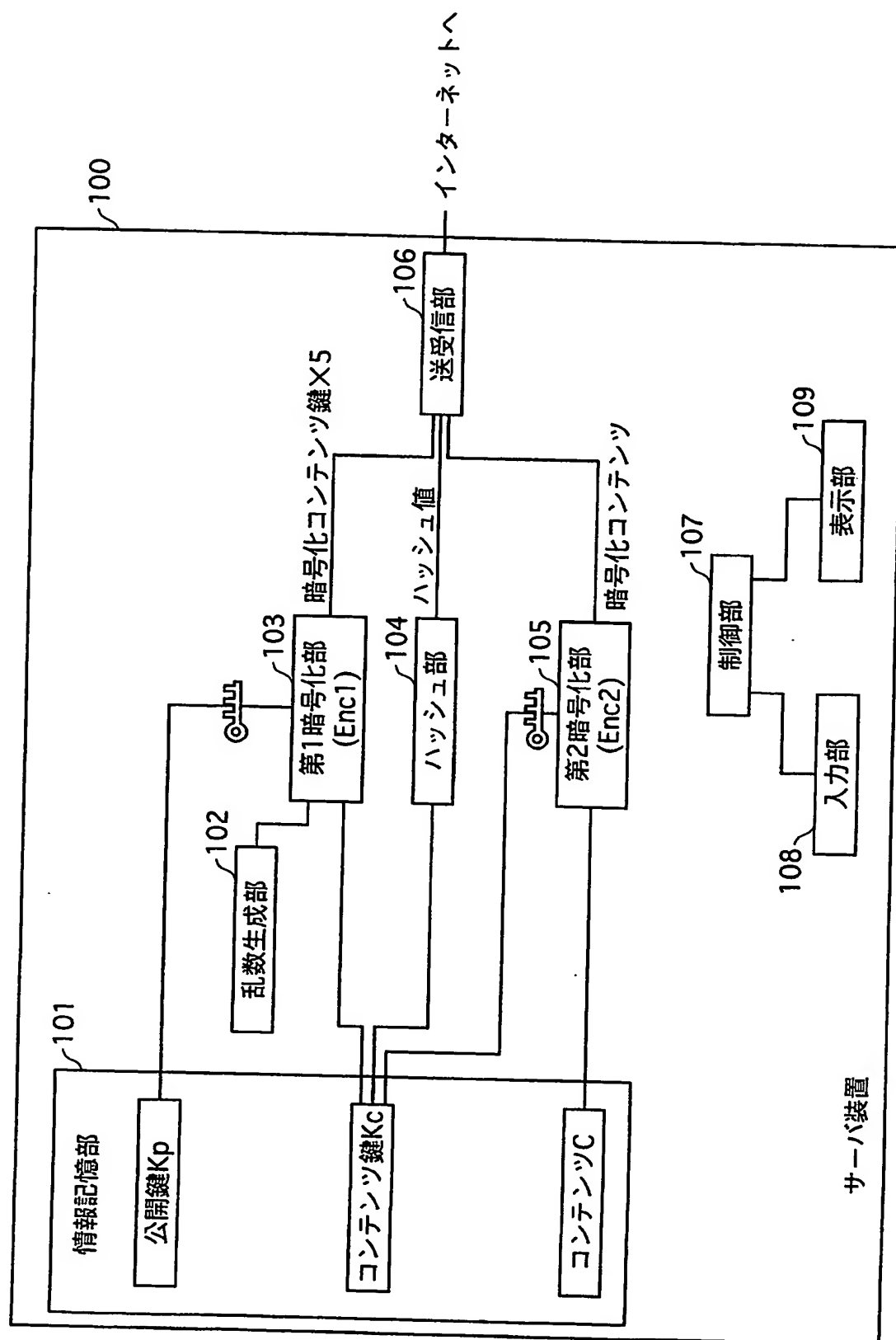
【書類名】

図面

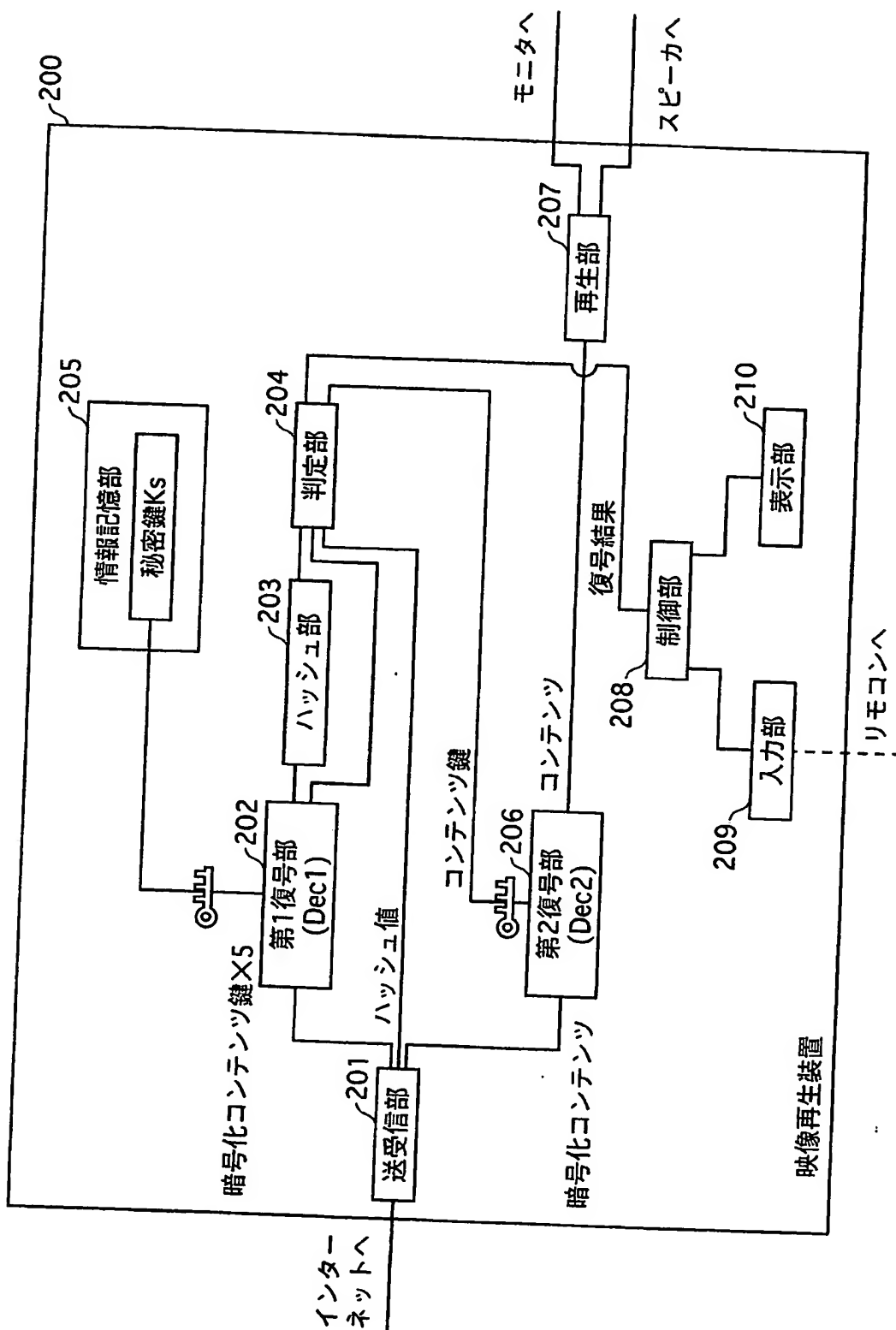
【図 1】



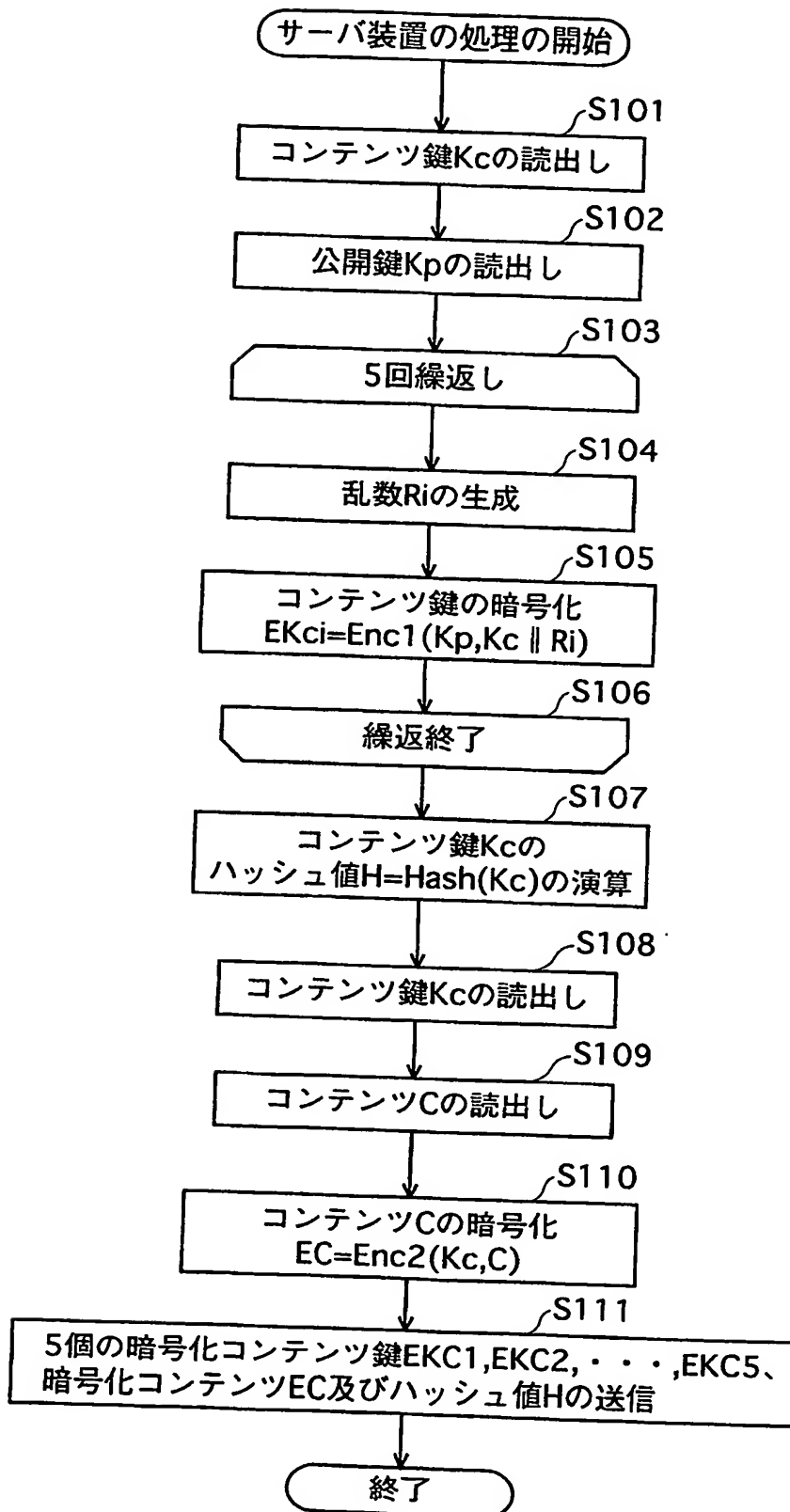
【図 2】



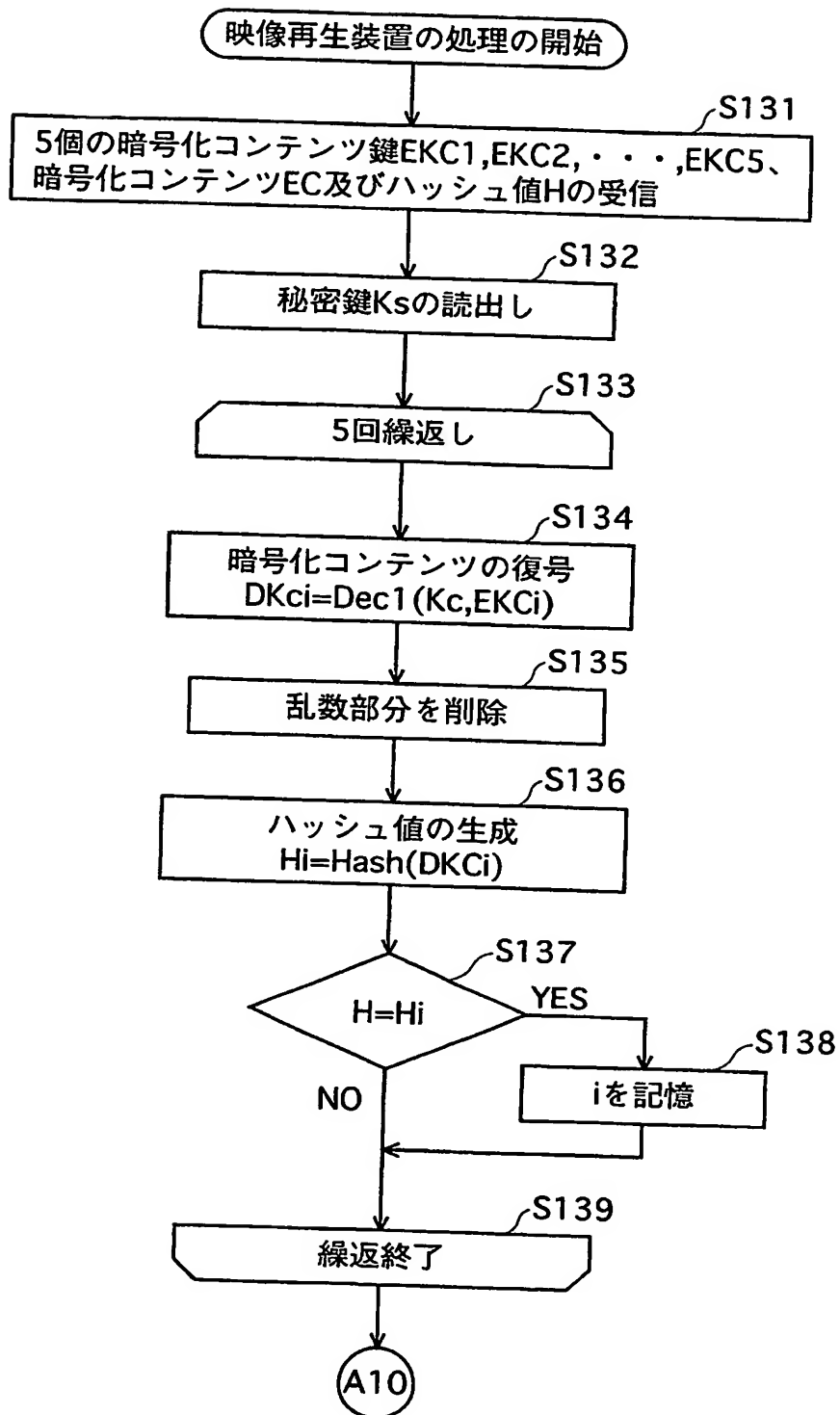
【図 3】



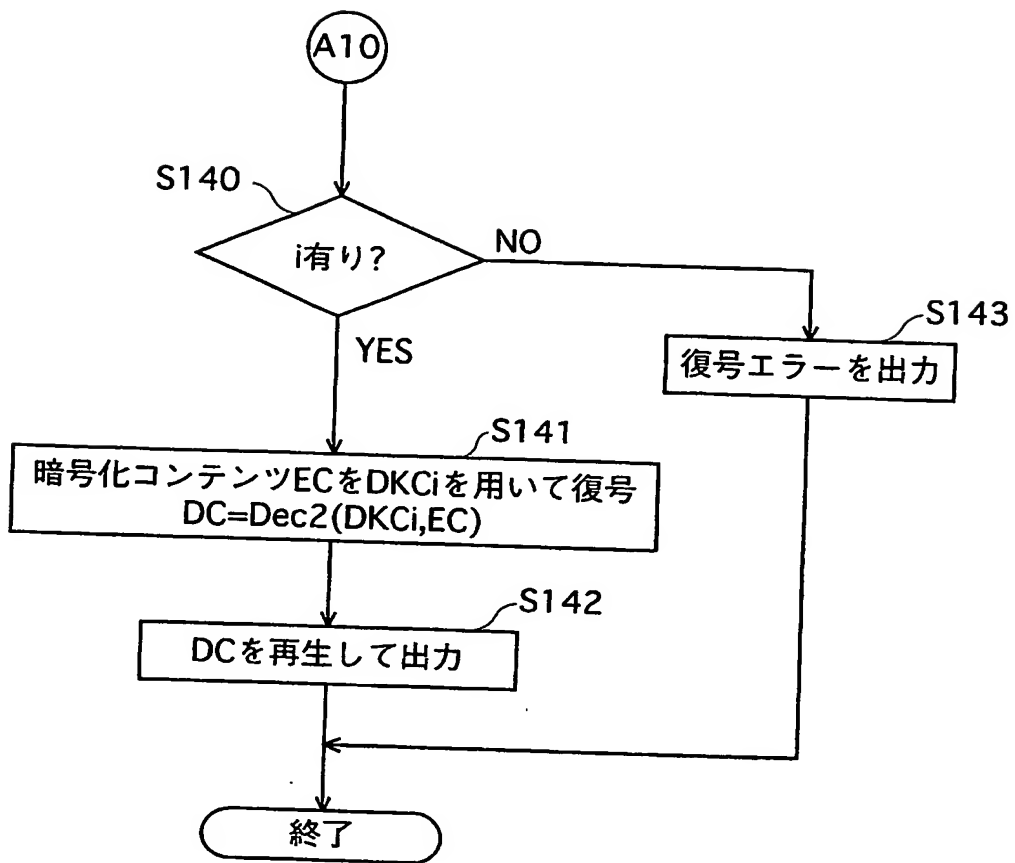
【図 4】



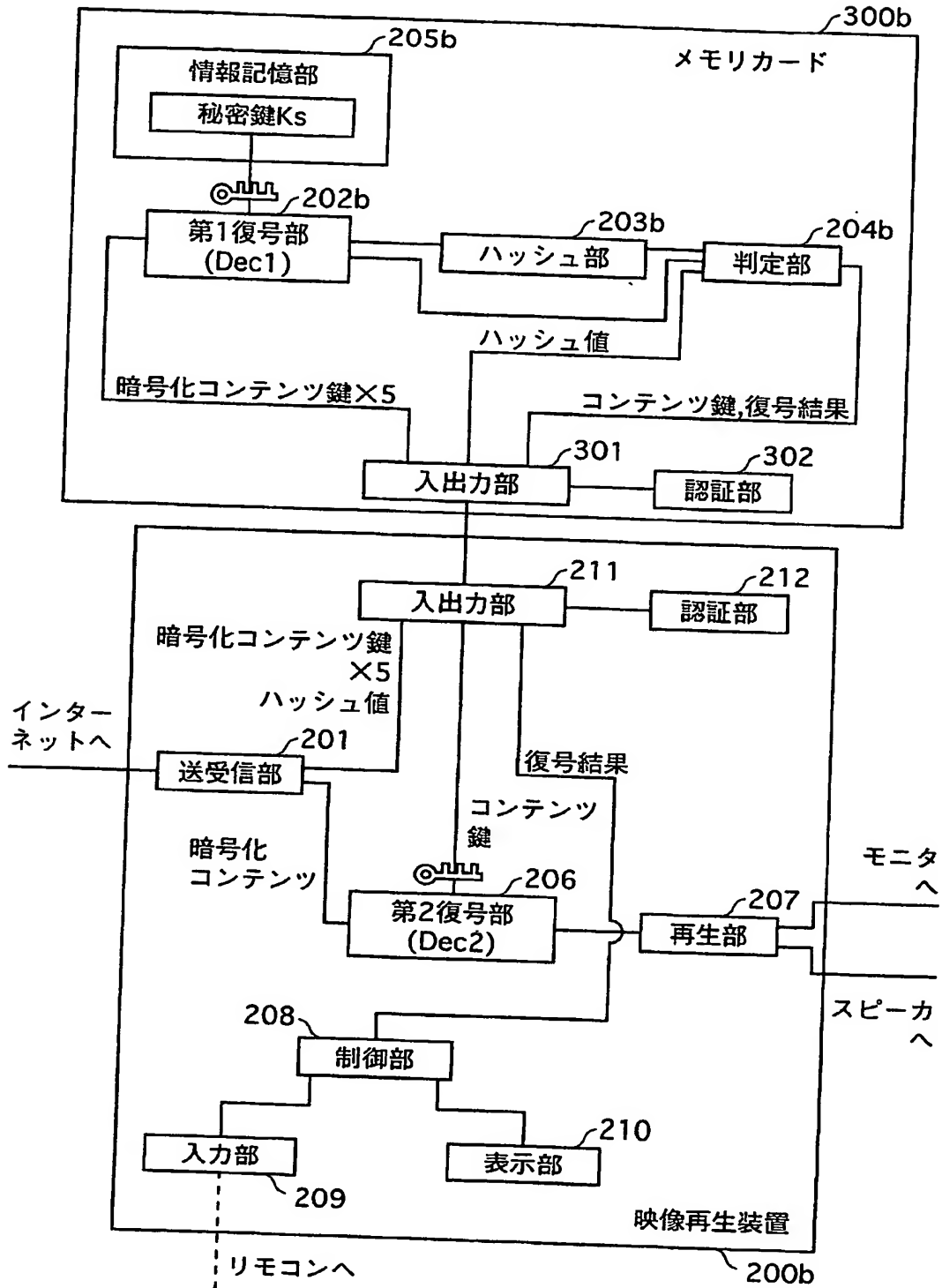
【図 5】



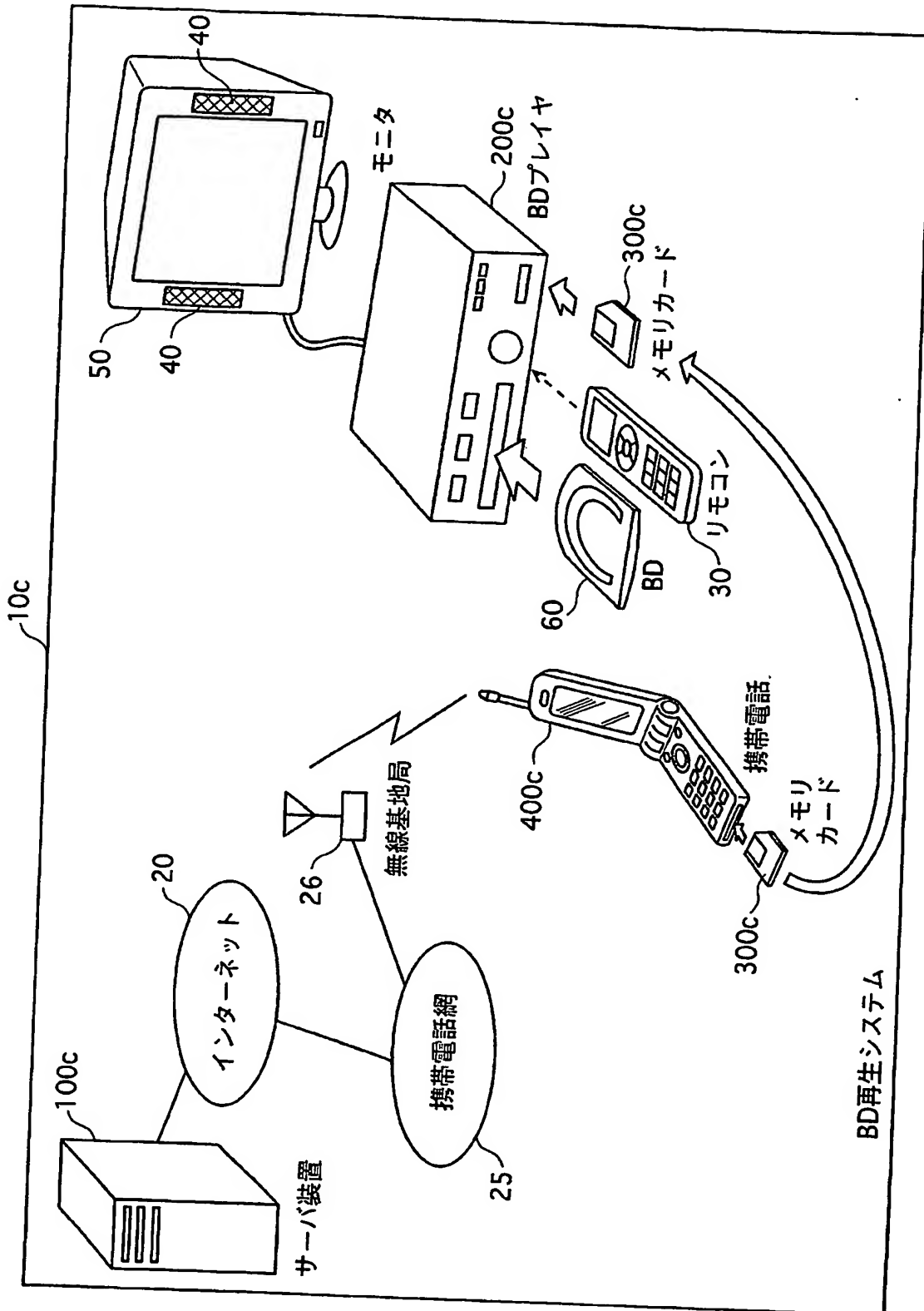
【図 6】



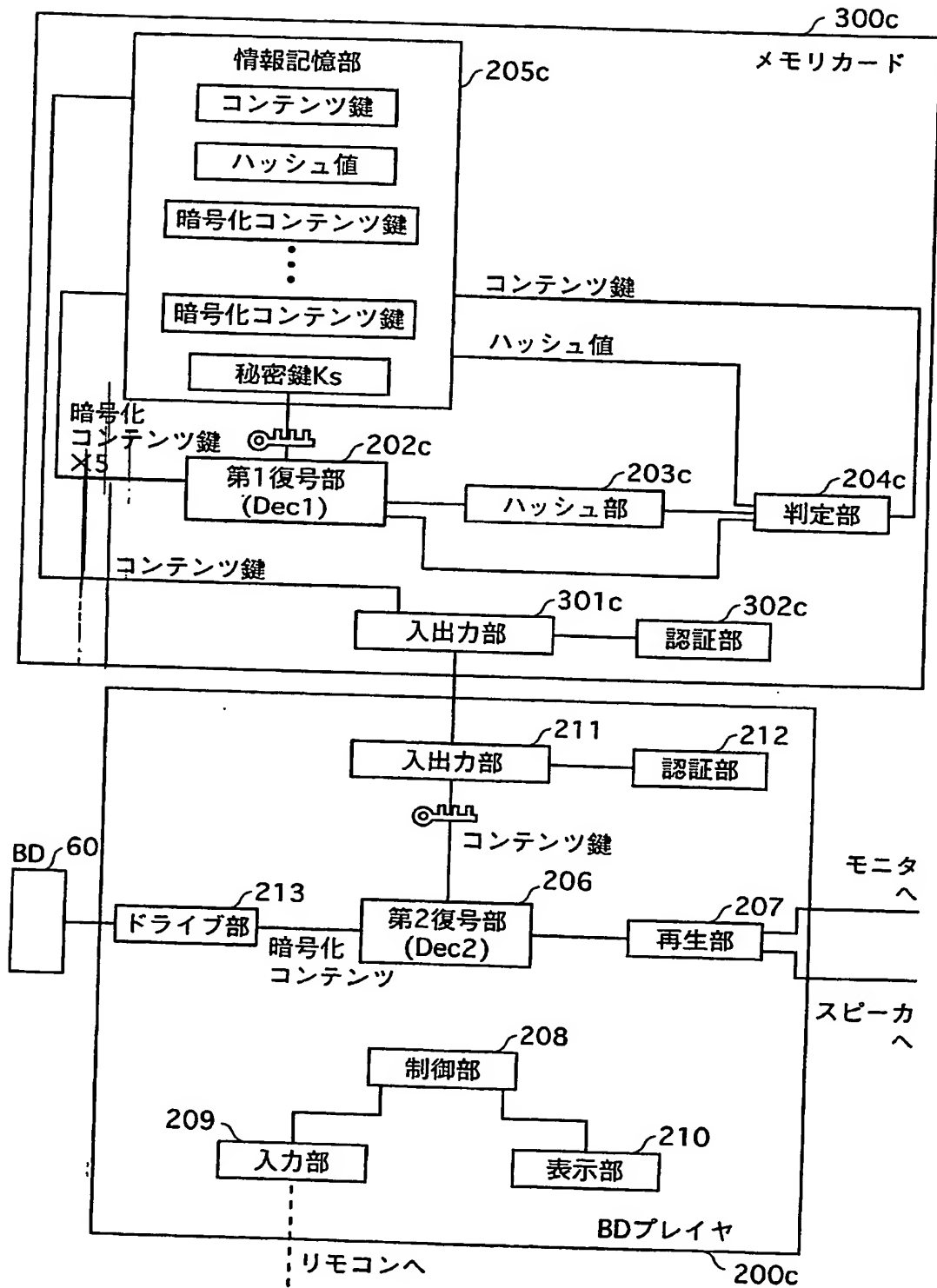
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 再送要求による攻撃を回避することができる暗号送信装置及び暗号受信装置を提供する。

【解決手段】 サーバ装置は、コンテンツ鍵を5回暗号化して5個の暗号化コンテンツ鍵を生成し、コンテンツ鍵のハッシュ値を算出し、5個の暗号化コンテンツ鍵とハッシュ値とを送信する。映像再生装置は、5個の暗号化コンテンツ鍵とハッシュ値とを受信し、5個の暗号化コンテンツ鍵を復号してそれぞれコンテンツ鍵を生成し、生成したコンテンツ鍵のハッシュ値をそれぞれ算出し、算出したハッシュ値と受信したハッシュ値とを比較する。1組でも一致すれば、対応するコンテンツ鍵を正しいものとみなす。5組の全てで一致しなければ、復号エラーとみなす。

【選択図】 図3

特願 2003-167374

ページ: 1/E

出願人履歴情報

識別番号

[000005821]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住所

大阪府門真市大字門真1006番地

氏名

松下電器産業株式会社